



New and Changed Information

- [New and Changed Information](#), on page 1

New and Changed Information



Note Cisco ISE Release 3.4 and the corresponding guides are available in a phased rollout. Until the software becomes generally available, contact your Cisco account manager to request this release. Upon completion of the phased rollout, Cisco ISE Release 3.4 and the corresponding guides will be made generally available to all customers.

The following table summarizes the new and changed features and tells you where they are documented.

Table 1: New and Changed Features in Cisco ISE Release 3.4

Feature	Description
Cisco ISE Resiliency	From Cisco ISE Release 3.4, the Excessive RADIUS Network Device Communication and Excessive Endpoint Communication alarms have been added to maintain the resiliency of Cisco ISE. See Cisco ISE Alarms .
Configure Debug Log Settings	You can configure the maximum file size and the maximum number of files allowed for each debug log component. You can also specify the date and time after which these values must be reset to default. See Configure Debug Log Settings .

Feature	Description
Create a URL Pusher pxGrid Direct Connector Type	<p>You can create a pxGrid Direct connector using the Cisco ISE GUI. There are two types of pxGrid Direct connector types: URL Fetcher and URL Pusher. From Cisco ISE Release 3.4, you can choose between a URL Fetcher pxGrid Direct connector type or a URL Pusher pxGrid Direct connector type. You can use the pxGrid Direct Push APIs to push endpoint data to Cisco ISE.</p> <p>From Cisco ISE Release 3.4, you can also configure an authorization profile using connector attributes containing arrays.</p> <p>See Create a URL Pusher Connector Type.</p>
End of Support for Legacy IPsec (ESR)	<p>From Cisco ISE Release 3.4, Legacy IPsec (ESR) is not supported on Cisco ISE. All IPsec configurations on Cisco ISE will be Native IPsec configurations. We recommend that you migrate to native IPsec from legacy IPsec (ESR) before upgrading to Cisco ISE Release to avoid any loss of tunnel and tunnel configurations.</p> <p>See Migrate from Legacy IPsec to Native IPsec on Cisco ISE.</p>
Enforcing Domain Controller Selection with Priority	<p>You can now choose to override Cisco ISE's selection of domain controllers in case of a preferred domain controller failover. When this option is enabled, Cisco ISE overrides the existing priority values and selects the next domain controller in the preferred list in the order of input from left to right.</p> <p>See Configure Preferred Domain Controllers.</p>
Enhanced Password Security	<p>Cisco ISE now improves password security through the following enhancements:</p> <ul style="list-style-type: none"> • You can choose to hide the Show button for the following field values, to prevent them from being viewed in plaintext during editing: <ul style="list-style-type: none"> Under Network Devices, <ul style="list-style-type: none"> • RADIUS Shared Secret • Radius Second Shared Secret Under Native IPsec, <ul style="list-style-type: none"> • Pre-shared Key <p>See Configure Security Settings.</p> • To prevent the RADIUS Shared Secret and Second Shared Secret from being viewed in plaintext during network device import and export, a new column with the header PasswordEncrypted:Boolean(true false) has been added to the Network Devices Import Template Format. No field value is required for this column. <p>See Network Devices Import Template Format.</p>

Feature	Description
On-demand pxGrid Direct Data Synchronization using Sync Now	<p>From Cisco ISE Release 3.4, you can use the Sync Now feature to perform on-demand synchronization of data from pxGrid Direct connectors. You can perform both full and incremental syncs on-demand. On-demand data synchronization can be performed through the Cisco ISE GUI or using OpenAPI.</p> <p>See On-demand pxGrid Direct Data Synchronization using Sync Now.</p>
Option to Add Identity Sync After Creating Duo Connection	<p>If you do not want to configure user data synchronization between Active Directory and Duo while creating a Duo connection, click Skip in the Identity Sync page. You will be taken to the Summary page directly.</p> <p>After you create a Duo connection, you can add identity sync configurations at any time.</p> <p>See Integrate Cisco Duo With Cisco ISE for Multifactor Authentication.</p>
Per-user Dynamic Access Control List Behavior Change	<p>While evaluating authorization profiles with per-user dynamic access control lists (DACLS), if a DACL does not exist in Cisco ISE configuration, authorization will fail, and Cisco ISE will send an Access-Reject response to that user. You can view this information in the Live Log Details page and the AAA Diagnostics report. From Cisco ISE Release 3.4 onwards, an authorization failure alarm is also displayed in the Alarms dashlet in the Cisco ISE dashboard.</p> <p>See Downloadable ACLs.</p>
Support for Multiple Cisco Application Centric Infrastructure Connectors	<p>Cisco ISE enables you to create and enforce consistent access policies across multiple domains. Cisco ISE can share the SGTs and SGT bindings with Cisco Application Centric Infrastructure (Cisco ACI). Cisco ISE can also learn the endpoint groups (EPGs), endpoint security groups (ESGs), and endpoint information from Cisco ACI. You can add multiple Cisco ACI connections to Cisco ISE.</p> <p>You can configure rules to manage the learned context in Cisco ISE and to optimize the context flows between Cisco ISE and Cisco ACI connectors.</p> <p>Cisco ISE supports Cisco ACI Multi-Tenant, and Multi-Virtual Routing and Forwarding deployments. You can define multi-fabrics through multiple connections. This integration supports multi-pod and individual Cisco ACI fabrics.</p> <p>See Connect Cisco Application Centric Infrastructure with Cisco ISE.</p>

Feature	Description
pxGrid Direct Support for Arrays in Dictionary Groups for Authorization Policy	<p>From Cisco ISE Release 3.4, you can also use pxGrid Direct Connector data with arrays as dictionary attributes to configure an authorization policy. The operators “Contains” or “Matches” (in case of REGEX) must be used while configuring the policy. The operators ”Equals” and “In” will not work when there are arrays. Multiple attributes can be nested using "AND" or "OR" conditions.</p> <p>See Configure Authorization Policies.</p>
RADIUS Suppression and Reports Enhancement	<p>From Cisco ISE Release 3.4, the RADIUS Suppression and Reports have been enhanced to facilitate easier RADIUS (Administration > System > Settings > Protocols > RADIUS > RADIUS Settings) configurations.</p> <p>See RADIUS Settings.</p>
Support for Transport Gateway Removed	<p>Cisco ISE no longer supports Transport Gateway. The following Cisco ISE features used Transport Gateway as a connection method:</p> <ul style="list-style-type: none"> • Cisco ISE Smart Licensing <p>If you use Transport Gateway as the connection method in your smart licensing configuration, you must edit the setting before you upgrade to Cisco ISE Release 3.4. You must choose a different connection method as Cisco ISE Release 3.4 does not support Transport Gateway. If you update to Cisco ISE Release 3.4 without updating the connection method, your smart licensing configuration is automatically updated to use the Direct HTTPS connection method during the upgrade process. You can change the connection method at any time after the upgrade.</p> • Cisco ISE Telemetry <p>Transport Gateway is no longer available as a connection method when using Cisco ISE Telemetry. The telemetry workflow is not impacted by this change.</p>

Feature	Description
TLS 1.3 Support for Cisco ISE Workflows	<p>Cisco ISE Release 3.4 allows TLS 1.3 to communicate with peers for the following workflows:</p> <ul style="list-style-type: none">• Cisco ISE is configured as an EAP-TLS server• Cisco ISE is configured as a TEAP server <p>Attention TLS 1.3 support for Cisco ISE configured as a TEAP server has been tested under internal test conditions because at the time of Cisco ISE Release 3.4, TEAP TLS 1.3 is not supported by any available client OS.</p> <ul style="list-style-type: none">• Cisco ISE is configured as a secure TCP syslog client <p>See Configure Security Settings.</p>

